FORM PTO-1390 (REV. 5-93)

U.S. DEPARTMENT OF COMMERCE
PATENT AND TRADEMARK OFFICE

JC04 Rec'd PCT/PTO 09 APR 2001

ATTORNEY'S DOCKET NUMBER
2345/149

TRANSMITTAL LETTER TO THE UNITED STATES DESIGNATED/ELECTED OFFICE (DO/EO/US) CONCERNING A FILING UNDER 35 U.S.C. 371

U.S. APPLICATION NO. (If known, see 37 CFR 1.5)
09/807176

INTERNATIONAL APPLICATION NO.	INTERNATIONAL FILING DATE	PRIORITY DATE CLAIMED:
PCT/EP99/07052	**22 September 1999 (22.09.99)**	**9 October 1998 (09.10.98)**

TITLE OF INVENTION
METHOD FOR ESTABLISHING A COMMON KEY BETWEEN A CENTRAL STATION AND A GROUP OF SUBSCRIBERS

APPLICANT(S) FOR DO/EO/US
Joerg SCHWENK

Applicant(s) herewith submits to the United States Designated/Elected Office (DO/EO/US) the following items and other information

1. ☒ This is a **FIRST** submission of items concerning a filing under 35 U.S.C. 371.
2. ☐ This is a **SECOND** or **SUBSEQUENT** submission of items concerning a filing under 35 U.S.C. 371.
3. ☒ This is an express request to begin national examination procedures (35 U.S.C. 371(f)) immediately rather than delay examination until the expiration of the applicable time limit set in 35 U.S.C. 371(b) and PCT Articles 22 and 39(1).
4. ☒ A proper Demand for International Preliminary Examination was made by the 19th month from the earliest claimed priority date.
5. ☒ A copy of the International Application as filed (35 U.S.C. 371(c)(2))
   a. ☐ is transmitted herewith (required only if not transmitted by the International Bureau).
   b. ☒ has been transmitted by the International Bureau.
   c. ☐ is not required, as the application was filed in the United States Receiving Office (RO/US)
6. ☒ A translation of the International Application into English (35 U.S.C. 371(c)(2)).
7. ☒ Amendments to the claims of the International Application under PCT Article 19 (35 U.S.C. 371(c)(3))
   a. ☐ are transmitted herewith (required only if not transmitted by the International Bureau).
   b. ☐ have been transmitted by the International Bureau.
   c. ☐ have not been made; however, the time limit for making such amendments has NOT expired.
   d. ☒ have not been made and will not be made.
8. ☐ A translation of the amendments to the claims under PCT Article 19 (35 U.S.C. 371(c)(3)).
9. ☒ An oath or declaration of the inventor(s) (35 U.S.C. 371(c)(4)) UNSIGNED.
10. ☒ A translation of the annexes to the International Preliminary Examination Report under PCT Article 36 (35 U.S.C. 371(c)(5)).

Items 11. to 16. below concern other document(s) or information included:

11. ☐ An Information Disclosure Statement under 37 CFR 1.97 and 1.98.
12. ☐ An assignment document for recording. A separate cover sheet in compliance with 37 CFR 3.28 and 3.31 is included.
13. ☒ A **FIRST** preliminary amendment.
    ☐ A **SECOND** or **SUBSEQUENT** preliminary amendment.
14. ☒ A substitute specification and marked-up version of specification.
15. ☐ A change of power of attorney and/or address letter.
16. ☒ Other items or information: International Search Report, Preliminary Examination Report, and Form PCT/RO/101.

Express Mail No.:EL594612691US

U.S. APPLICATION NO if known, see 37 CFR 1.5	INTERNATIONAL APPLICATION NO	ATTORNEY'S DOCKET NUMBER
09/807176	PCT/EP99/07052	2345/149

17. ☒ The following fees are submitted:	CALCULATIONS | PTO USE ONLY
Basic National Fee (37 CFR 1.492(a)(1)-(5)):	
Search Report has been prepared by the EPO or JPO $860.00	
International preliminary examination fee paid to USPTO (37 CFR 1.482) $690.00	
No international preliminary examination fee paid to USPTO (37 CFR 1.482) but international search fee paid to USPTO (37 CFR 1.445(a)(2)) $710.00	
Neither international preliminary examination fee (37 CFR 1.482) nor international search fee (37 CFR 1.445(a)(2)) paid to USPTO $1,000.00	
International preliminary examination fee paid to USPTO (37 CFR 1.482) and all claims satisfied provisions of PCT Article 33(2)-(4) $100.00	

ENTER APPROPRIATE BASIC FEE AMOUNT =				$ 860	
Surcharge of $130.00 for furnishing the oath or declaration later than ☐ 20 ☐ 30 months from the earliest claimed priority date (37 CFR 1.492(e)).				$	
Claims	Number Filed	Number Extra	Rate		
Total Claims	1 - 20 =	0	X $18.00	$0	
Independent Claims	1 - 3 =	0	X $80.00	$0	
Multiple dependent claim(s) (if applicable)			+ $270.00	$	
TOTAL OF ABOVE CALCULATIONS =				$860	
Reduction by 1/2 for filing by small entity, if applicable. Verified Small Entity statement must also be filed. (Note 37 CFR 1.9, 1.27, 1.28).				$	
SUBTOTAL =				$860	
Processing fee of $130.00 for furnishing the English translation later the ☐ 20 ☐ 30 months from the earliest claimed priority date (37 CFR 1.492(f)). +				$	
TOTAL NATIONAL FEE =				$860	
Fee for recording the enclosed assignment (37 CFR 1.21(h)). The assignment must be accompanied by an appropriate cover sheet (37 CFR 3.28, 3.31). $40.00 per property +				$	
TOTAL FEES ENCLOSED =				$860	
				Amount to be refunded	$
				charged	$

a. ☐ A check in the amount of $_____ to cover the above fees is enclosed.

b. ☒ Please charge my Deposit Account No. 11-0600 in the amount of $860.00 to cover the above fees. A duplicate copy of this sheet is enclosed.

c. ☒ The Commissioner is hereby authorized to charge any additional fees which may be required, or credit any overpayment to Deposit Account No. 11-0600. A duplicate copy of this sheet is enclosed.

NOTE: Where an appropriate time limit under 37 CFR 1.494 or 1.495 has not been met, a petition to revive (37 CFR 1.137(a) or (b)) must be filed and granted to restore the application to pending status.

By Reg No 35,952

SIGNATURE

SEND ALL CORRESPONDENCE TO:
Kenyon & Kenyon
One Broadway
New York, New York 10004
Telephone No. (212)425-7200
Facsimile No. (212)425-5288
CUSTOMER NO. 26646

Richard L. Mayer, Reg. No. 22,490
NAME

4/9/01
DATE

26646
PATENT TRADEMARK OFFICE

[2345/149]

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Inventor(s)	:	Joerg SCHWENK
Serial No.	:	To Be Assigned
Filed	:	Herewith
For	:	METHOD FOR ESTABLISHING A COMMON KEY BETWEEN A CENTRAL STATION AND A GROUP OF SUBSCRIBERS
Examiner	:	To Be Assigned
Art Unit	:	To Be Assigned

Assistant Commissioner for Patents
Washington, D.C. 20231

PRELIMINARY AMENDMENT

SIR:

Kindly amend the above-identified application before examination, as set forth below.

IN THE TITLE:

Please replace the title with the following:

--METHOD FOR ESTABLISHING A COMMON KEY BETWEEN A CENTRAL STATION AND A GROUP OF SUBSCRIBERS--.

IN THE SPECIFICATION:

Please amend the specification, including abstract, pursuant to the attached substitute specification. Also attached is a red-lined copy of the specification, indicating deleted and added sections. No new matter has been added.

IN THE CLAIMS:

Please cancel original claim 1 and please cancel substitute claim 1, without prejudice.

Please add the following new claim:

2. (New) A method for establishing a common key k between a central station Z and a group of subscribers T1-Tn, comprising:

providing a publicly known mathematical group G and an element $g \in G$ of a high order in the group G, so that for the group G and the element g a calculation of a discrete logarithm is essentially impossible;

using a predetermined threshold method, wherein a random number i is generated by each subscriber Ti of the group of subscribers T1-Tn, and from the element $g \in G$ and the random number i, the value g^i is calculated by each subscriber Ti of the group of subscribers T1-Tn and transmitted to the central station Z; in the central station Z, a random number z is generated; from the random number z and the values g^i, the values $(g^i)^z$ in the group G are calculated, from the values $(g^i)^z$, n shares $(s_1,\ldots,s_n)$ of the threshold method are derived, and from the shares $(s_1,\ldots,s_n)$, an (n,2n-1) threshold method is constructed, a secret of the (n,2n-1) threshold method being the key k to be established; in the central station Z, n-1 further shares $(s_{n+1},\ldots s_{2n-1})$ differing from shares $(s_1,\ldots,s_n)$ are calculated together with the value g^z in the group G and are transmitted to the group of subscribers T1-Tn; and for each subscriber Ti of the group of subscribers T1-Tn, the key k to be established is reconstructed so that from the value g^z transmitted by the central station Z and the random number i of each subscriber Ti of the group of subscribers T1-Tn, the value $(g^z)^i$ in the group G is calculated, and that from the resulting value, applying the (n,2n-1) threshold method, the share s_i is derived, and that using the share s_i and the further shares $(s_{n+1},\ldots s_{2n-1})$ transmitted by the central station Z, the key k is reconstructed.

REMARKS

This Preliminary Amendment cancels, without prejudice, original claim 1 and substitute claim 1 in the underlying PCT Application No. PCT/EP99/07052, and adds new claim 2. The new claim conforms to U.S. Patent and Trademark Office rules and does not add new matter to the application.

The amendments to the specification and abstract reflected in the substitute specification are to conform the specification and abstract to U.S. Patent and Trademark Office rules and to introduce changes made in the underlying PCT application, and do not introduce new matter into the application.

The underlying PCT Application No. PCT/EP99/07052 includes an International Search Report, issued January 24, 2000, a copy of which is included. The Search Report includes a list of documents that were considered by the Examiner in the underlying PCT application.

The underlying PCT Application No. PCT/EP99/07052 also includes an International Preliminary Examination Report, issued October 5, 2000, a copy of which is included, including a translation.

Applicants assert that the present invention is new, non-obvious, and useful. Prompt consideration and allowance of the claims are respectfully requested.

Respectfully Submitted,

KENYON & KENYON

Dated: 4/9/01

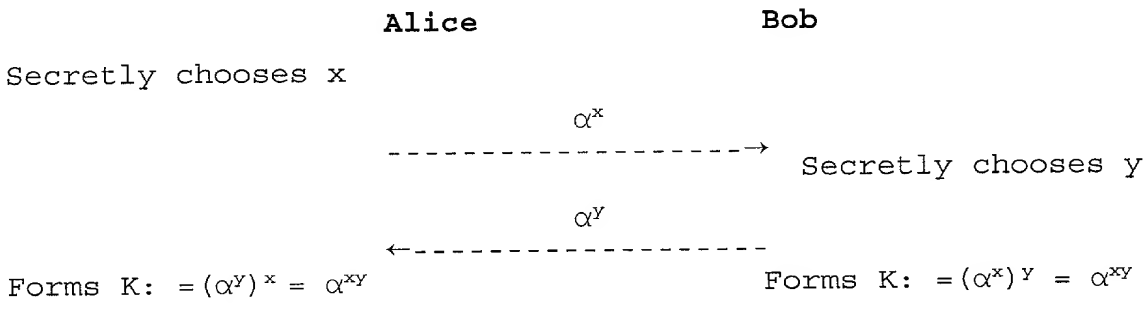
By: RJM 35,952
Richard L. Mayer
Reg. No. 22,490

One Broadway
New York, NY 10004
(212) 425-7200
(212) 425-5288
CUSTOMER NO. 26646

METHOD FOR ESTABLISHING A COMMON KEY BETWEEN A CENTRAL STATION AND A GROUP OF SUBSCRIBERS

The present invention is directed to a method for establishing a common key between a central station and a group of subscribers according to the definition of the species in the independent claim. There are many diverse encryption methods in the related art, and these methods have gained in commercial importance. They are used for transmitting information over generally accessible transmission media. However, only the owner of a cryptographic key is able to read this information in plain text.

A known method for establishing a common key via insecure communication channels is, for example, the W. Diffie and W. Hellman method (see DH method, W. Diffie and M. Hellmann; see "New Directions in Cryptography", IEEE Transactions on Information Theory, IT-22(6):644-654, November 1976). The Diffie-Hellmann key exchange [DH76] is based on the fact that it is virtually impossible to calculate logarithms modulo a large prime number p. Alice and Bob take advantage of this fact in the example illustrated below, by each secretly choosing a number x and y, respectively, smaller than p (and prime to p-1). They then send each other (consecutively or simultaneously) the x-th (and, respectively, y-th) power of a publicly known number α. From the received powers, they are able to calculate a common key $K:=\alpha^{xy}$ by again performing an exponentiation with x and y, respectively. An attacker, who sees only α^x and α^y, is not able to calculate K therefrom. (The only method known today to do so would involve first calculating the logarithm, e.g. of α^x to the base α modulo p, and then raising α^y to that power.)



Example of the Diffie-Helmann key exchange

The problem that exists in the case of the DH key exchange is that Alice does not know whether she is actually communicating with Bob or with an impostor. In IPSec, this problem is solved by the use of public key certificates in which the identity of a subscriber is linked to a public key by a trustworthy authority. In this way, the identity of a conversation partner is can be verified.

The DH key exchange can also be implemented using other mathematical structures, such as finite fields $GF(2^n)$ or elliptical curves. With such alternatives, one can improve performance.

However, this method is only suitable for agreement of a key between two subscribers.

Various attempts have been made to extend the DH method to three or more subscribers (DH groups). M. Steiner, G. Tsudik, and M. Waidner provide an overview of the state of the art in "Diffie-Hellman Key Distribution Extended to Group Communication", Proc. 3rd ACM Conference on Computer and Communications Security, March 1996, New Delhi, India.

The following table illustrates an example where the DH method is extended to three subscribers A, B and C (in each case, calculations are mod p):

	A→B	B→C	C→A
1st round	g^a	g^b	g^c
2nd round	g^{ca}	g^{ab}	g^{bc}

Once these two rounds have been carried out, each of the subscribers is able to calculate the secret key g^{abc} mod p.

In all of these extensions, at least one of the following problems occurs:

- The subscribers must be arranged in a certain manner, in the above example, for instance, in a circle.
- The subscribers have no influence on the key selection vis-à-vis the central station.
- The number of rounds is dependent on the number of subscribers.

As a general rule, these methods are difficult to implement and require substantial computational outlay.

Another method for establishing a common key is known from the German Patent DE 195 38 385.0. In this method, however, the central station must know the secret keys of the subscribers.

An approach is also known from Burmester, Desmedt, "A Secure and Efficient Conference Key Distribution System", Proc. EUROCRYPT'94, Springer LNCS, Berlin 1994, where two rounds are required to generate the key, it being necessary to send n communications of a length of p = approx. 1000 bits through the central station for n subscribers in the second round.

A cryptographic method described as the (n,t) threshold method is also known. In an (n,t) threshold method, a key k can be decomposed into t parts (referred to as shadows), in such a way that this key k can be reconstructed from any n of the t shadows (see Beutelspacher, Schwenk, Wolfenstetter: *Moderne Verfahren der Kryptographie* (2nd edition), Vieweg Publishers, Wiesbaden, 1998).

It is intended that the present method for generating a common key between a central station and a group of at least three subscribers have the same security standards as the DH method. In this context, however, the method should be simple to implement and require minimal computational outlay. It should be so conceived that there is no need, in the process, for the subscribers' secret keys to be made known to the central station.

The method according to the present invention is equal to this task. It is based on the same mathematical structures as the DH method and, therefore, has comparable security features. In comparison to the group DH methods proposed in known methods heretofore, it is substantially more efficient with respect to computational outlay and communication requirements.

The operating principle of the method according to the present invention is elucidated in the following. In this instance, the central station is denoted by Z, defined subscribers in the method by T1-Tn, and every single subscriber, who is not specifically named, by Ti. The publicly known components of the method include a publicly known mathematical group G, preferably the multiplicative group of all integral numbers modulo a large prime number p, and an element g of the group G, preferably a number $0<g<p$ having a high multiplicative order. For group G, however, other suitable mathematical structures can also be used, e.g., the multiplicative group of a finite field, or the group of the points of an elliptical curve.

The method is carried out in three work steps.
In the first step, a communication in the form $(Ti, g^i \bmod p)$ is sent by each subscriber Ti to the central station, i being a random number of subscriber Ti selected by a random number generator.

In the second work step, in central station Z:

- A random number z is generated, and the number $(g^i)^z$ mod p is calculated for each subscriber Ti.
- From these n numbers, n shares are then differentiated for n subscribers in central station Z, using a generally known (n, 2n-1) threshold method.
- n-1 further shares s^1-s^{n-1} are selected in central station Z and sent, together with the number g^z mod p, to all subscribers Tl-Tn.

In the third work step, the common key k is calculated for each subscriber Ti,

- $(g^z)^i$ mod p = $(g^i)^z$ mod p being calculated;
- from this, a share of the threshold method being differentiated; and
- on the basis of this share and $s^1,...s^{n-1}$, common key k being determined as the secret.

On the basis of a practical example, the method according to the present invention is elucidated in the following for three subscribers A, B, and C, as well as a central station Z. However, the number of subscribers can be increased to any desired number. In this example, the length of number p is 1024 bits; g has a multiplicative order of at least 2^{160}.

The method in accordance with the present invention is carried out in accordance with the following method steps:

1. Subscribers A, B and C send g^a mod p, g^b mod p and g^c mod p to central station Z.
2. g^{az} mod p, g^{bz} mod p and g^{cz} mod p are calculated in central station Z, in each case the 128 least significant bits thereof being used as shares s_A, s_B and, respectively, s_C. In central station Z, applying the (n,2,-1) threshold method, a 2^{nd} degree polynomial P(x), which passes through points $(1,s_A)$, $(2,s_B)$, and $(3,s_C)$ and is uniquely defined by these points, is calculated over a finite field GF(2^{128}). Common key k is the point of intersection of this polynomial with the y-axis, i.e., k; =P(0). Central station Z transmits g^z

mod p, s_1;=P(4) and s_2;=P(5) to subscribers A, B and C.

3. For subscriber A, $(g^z)^a$ mod p is calculated. In the result, subscriber A having the 128 least significant bits of this value receives share s_A, which, together with shares s_1 and s_2 is sufficient to determine polynomial P'(x) and, thus, also key k. One proceeds analogously for subscribers B and C.

The method described above makes do with the minimum number of two rounds between subscribers T1-Tn and central station Z. In contrast to the Burmester and Desmedt approach, the outlay for character strings to be transmitted by the central station to the n subscribers can be reduced in the second round to a length of 128 bits per subscriber.

What is claimed is:

1. A method for establishing a common key k between a central station Z and a group of subscribers T1-Tn, including a publicly known mathematical group G and an element gϵG of a high order in the group G, so that for group G and the element g, the calculation of the discrete logarithm is virtually impossible, wherein

a) a random number (i) is generated by each subscriber (Ti) and, from the known element gϵG and the random number (i) in question, the value (g^i) is calculated by each subscriber (Ti) and transmitted to the central station (Z);

b) in the central station (Z), a random number (z) is generated; from the random number (z) and the received values (g^i), the values $(g^i)^z$ in G are calculated; from these values, n shares ($s_1,\ldots,s_n$) of a threshold method are derived; and from the shares ($s_1,\ldots,s_n$), a (n,2,-1) threshold method is constructed, the secret implicitly given by this method being the key (k) to be established; in the central station (Z), n-1 further shares ($s_{n+1},\ldots s_{2n-1}$) differing from shares ($s_1,\ldots,s_n$) are calculated, together with the value g^z in G, and transmitted to the subscribers (T1-Tn); and

c) for each subscriber (Ti), the key (k) to be established is reconstructed in that, from the value (g^z) transmitted by the central station (Z), and the random number (i) of the subscriber (Ti) in question, the value for $(g^z)^1$ in G is calculated; that from the resulting value, applying a threshold method, the share (s_i) is derived, and that, on the basis of the share (s_i) and the shares ($s_{n+1},\ldots s_{2n-1}$) transmitted by the central station (Z), the key (k) is reconstructed with the aid of the (n,2,-

1) threshold method.

1. A Method for Establishing a Common Key Between a Central Station and a Group of Subscribers

2. Abstract

2.1. It is intended that the present method for generating a common key between a central station and a group of at least three subscribers exhibit the same standard of security as the DH method.

2.2. The method is based on a publicly known mathematical number group (G) and an element of the group $g \in G$ of a high order. Each of the n subscribers generates a random number (i), calculates the value of g^i in G, and transmits this value to the central station (Z). In the central station (Z), a random number (z) is likewise generated, and the values $(g^i)^z$ in G are calculated. From these values, the shares are derived on the basis of a threshold method and, from these, a (n,2n-1) threshold method is constructed. The central station (Z) transmits the generated shares, together with the values $(g^i)^z$, to the n subscribers, who, using the (n,2n-1) threshold method, can reconstruct the key (k).

2.3. The method in accordance with the present invention can be advantageously used for generating a cryptographic key for a group of a plurality, however of at least three, subscribers.

METHOD FOR ESTABLISHING A COMMON KEY BETWEEN A CENTRAL STATION AND A GROUP OF SUBSCRIBERS

Field of the Invention

The present invention is directed to a method for establishing a common key between a central station and a group of subscribers according to the definition of the species in the independent claim.

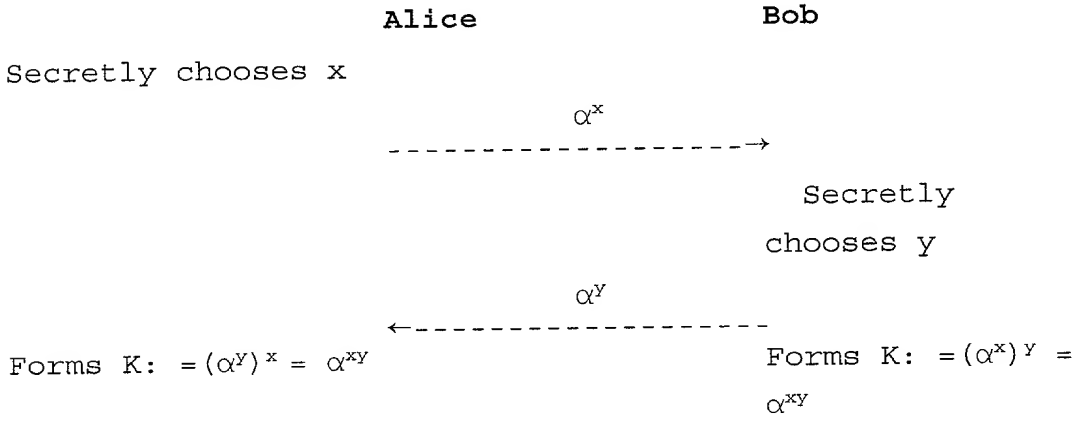
Background Information

There are many diverse encryption methods in the related art, and these methods have gained in commercial importance. They are used for transmitting information over generally accessible transmission media. However, only the owner of a cryptographic key is able to read this information in plain text.

A known method for establishing a common key via insecure communication channels is, for example, the W. Diffie and W. Hellman method (see DH method, W. Diffie and M. Hellmann; see "New Directions in Cryptography", IEEE Transactions on Information Theory, IT-22(6):644-654, November 1976).

The Diffie-Hellmann key exchange [DH76] is based on the fact that it is virtually impossible to calculate logarithms modulo a large prime number p. Alice and Bob take advantage of this fact in the example illustrated below, by each secretly choosing a number x and y, respectively, smaller than p (and prime to p-1). They then send each other (consecutively or simultaneously) the x-th (and, respectively, y-th) power of a publicly known number α. From the received powers, they are able

to calculate a common key $K:=\alpha^{xy}$ by again performing an exponentiation with x and y, respectively. An attacker, who sees only α^x and α^y, is not able to calculate K therefrom. (The method known today to do so would involve first calculating the logarithm, e.g. of α^x to the base α modulo p, and then raising α^y to that power.)



Example of the Diffie-Helmann key exchange

The problem that exists in the case of the DH key exchange is that Alice does not know whether she is actually communicating with Bob or with an impostor. In IPSec, this problem is solved by the use of public key certificates in which the identity of a subscriber is linked to a public key by a trustworthy authority. In this way, the identity of a conversation partner is can be verified.

The DH key exchange can also be implemented using other mathematical structures, such as finite fields $GF(2^n)$ or elliptical curves. With such alternatives, one can improve performance.

However, this method is only suitable for agreement of a key between two subscribers.

Various attempts have been made to extend the DH method

to three or more subscribers (DH groups). M. Steiner, G. Tsudik, and M. Waidner provide an overview of the state of the art in "Diffie-Hellman Key Distribution Extended to Group Communication", Proc. 3rd ACM Conference on Computer and Communications Security, March 1996, New Delhi, India.

The following table illustrates an example where the DH method is extended to three subscribers A, B and C (in each case, calculations are mod p):

	A→B	B→C	C→A
1st round	g^a	g^b	g^c
2nd round	g^{ca}	g^{ab}	g^{bc}

Once these two rounds have been carried out, each of the subscribers is able to calculate the secret key g^{abc} mod p.

In all of these extensions, at least one of the following problems occurs:

- The subscribers must be arranged in a certain manner, in the above example, for instance, in a circle.
- The subscribers have no influence on the key selection vis-à-vis the central station.
- The number of rounds is dependent on the number of subscribers.

As a general rule, these methods are difficult to implement and require substantial computational outlay.

Another method for establishing a common key is known from German Patent No. DE 195 38 385.0. In this method, however, the central station must know the secret keys of the subscribers.

Another approach is known from Burmester, Desmedt, "A Secure and Efficient Conference Key Distribution System", Proc. EUROCRYPT'94, Springer LNCS, Berlin 1994, where two rounds are required to generate the key, it being necessary to send n communications of a length of p = approx. 1000 bits through the central station for n subscribers in the second round.

A cryptographic method described as the (n,t) threshold method is also known. In an (n,t) threshold method, a key k can be decomposed into t parts (referred to as shadows), so that this key k can be reconstructed from any n of the t shadows (see Beutelspacher, Schwenk, Wolfenstetter: *Moderne Verfahren der Kryptographie* (2nd edition), Vieweg Publishers, Wiesbaden, 1998).

In IEEE Infocom '93, The Conference on Computer Communications Proceedings, Twelfth Annual Joint Conference of the IEEE Computer and Communications Societies, Networking: Foundation for the Future (cat. no. 93CH3264-9) (3/28/1993), vol. 3, pp. 1406-1413, "On the Design of Conference Key Distribution Systems for the Broadcasting Networks", a method is described for establishing a common key between a central station (chairman) and a group of n subscribers, where a threshold method is employed. In this approach, the central station (chairman) selects a common key. The method presupposes a secure channel between the chairman and the subscribers. A secure channel of this kind can be established, for example, using the DH method [DH76] indicated above, or a variant. However, for this, two communications are necessary for each subscriber, in order to negotiate a common key between the n subscribers and the central station (chairman), and to transmit a communication around the "public shadows".

Thus, altogether 2n+1 communications are required in order to establish the common key.

Summary of the Invention

The present invention provides a method for generating a common key between a central station and a group of at least three subscribers exhibit the same standard of security as the DH method. The method can be based on a publicly known mathematical number group (G) and an element of the group g∈G of a high order. Each of the n subscribers generates a random number (i), calculates the value of g^i in G, and transmits this value to the central station (Z). In the central station (Z), a random number (z) is likewise generated, and the values $(g^i)^z$ in G are calculated. From these values, the shares are derived on the basis of a threshold method and, from these, a (n,2n-1) threshold method is constructed. The central station (Z) transmits the generated shares, together with the values $(g^i)^z$, to the n subscribers, who, using the (n,2n-1) threshold method, can reconstruct the key (k). The method in accordance with the present invention can be used for generating a cryptographic key for three or more subscribers.

Detailed Description

The present invention provides a method for generating a common key between a central station and a group of at least three subscribers having the same security standards as the DH method. In this context, the method can be simple to implement and require minimal computational outlay.

The present invention is based, inter alia, on the same mathematical structures as the DH method and, therefore, has comparable security features. In comparison to the

group DH methods proposed in known methods heretofore, it is substantially more efficient with respect to computational outlay and communication requirements.

The operating principle of the method according to the present invention is elucidated in the following. In this instance, the central station is denoted by Z, defined subscribers in the method by T1-Tn, and every single subscriber, who is not specifically named, by Ti. The publicly known components of the method include a publicly known mathematical group G, preferably the multiplicative group of all integral numbers modulo a large prime number p, and an element g of the group G, preferably a number $0<g<p$ having a high multiplicative order. For group G, however, other suitable mathematical structures can also be used, e.g., the multiplicative group of a finite field, or the group of the points of an elliptical curve.

The method can be carried out in three steps. In a first step, a communication in the form (Ti, g^i mod p) can be sent by each subscriber Ti to the central station, i being a random number of subscriber Ti selected by a random number generator.

In a second work step, in central station Z:

- A random number z is generated, and the number $(g^i)^z$ mod p is calculated for each subscriber Ti.
- From these n numbers, n shares are then differentiated for n subscribers in central station Z, using a generally known (n, 2n-1) threshold method.
- n-1 further shares s^1-s^{n-1} are selected in central station Z and sent, together with the number g^z mod p, to all subscribers T1-Tn.

In a third work step, the common key k can be calculated for each subscriber Ti,- $(g^z)^i \bmod p = (g^i)^z \bmod p$ being calculated;

- from this, a share of the threshold method being differentiated; and
- on the basis of this share and $s^1,...s^{n-1}$, common key k being determined as the secret.

On the basis of a practical example, the method according to the present invention is elucidated in the following for three subscribers A, B, and C, as well as a central station Z. However, the number of subscribers can be increased to any desired number. In this example, the length of number p is 1024 bits; g has a multiplicative order of at least 2^{160}.

An embodiment of the method in accordance with the present invention can be carried out as follows:

- Subscribers A, B and C send $g^a \bmod p$, $g^b \bmod p$ and $g^c \bmod p$ to central station Z.
- $g^{az} \bmod p$, $g^{bz} \bmod p$ and $g^{cz} \bmod p$ are calculated in central station Z, in each case the 128 least significant bits thereof being used as shares S_A, S_B and, respectively, S_C. In central station Z, applying the (n,2,-1) threshold method, a 2^{nd} degree polynomial P(x), which passes through points $(1,s_A)$, $(2,s_B)$, and $(3,s_C)$ and is uniquely defined by these points, is calculated over a finite field $GF(2^{128})$. Common key k is the point of intersection of this polynomial with the y-axis, i.e., k; =P(0). Central station Z transmits $g^z \bmod p$, s_1;=P(4) and s_2;=P(5) to subscribers A, B and C.
- For subscriber A, $(g^z)^a \bmod p$ is calculated. In the result, subscriber A having the 128 least significant bits of this value receives share s_A, which, together with shares s_1 and s_2 is sufficient

to determine polynomial P'(x) and, thus, also key k. One proceeds analogously for subscribers B and C.

The method described above can use a minimum number of two rounds between subscribers T1-Tn and central station Z. In contrast to the Burmester and Desmedt approach, the outlay for character strings to be transmitted by the central station to the n subscribers can be reduced in the second round to a length of 128 bits per subscriber.

Abstract

The present invention provides a method for generating a common key between a central station and a group of subscribers, e.g., at least three subscribers, exhibit the same standard of security as the DH method.

METHOD FOR ESTABLISHING A COMMON KEY BETWEEN A CENTRAL STATION AND A GROUP OF SUBSCRIBERS

Field of the Invention

The present invention is directed to a method for establishing a common key between a central station and a group of subscribers according to the definition of the species in the independent claim.

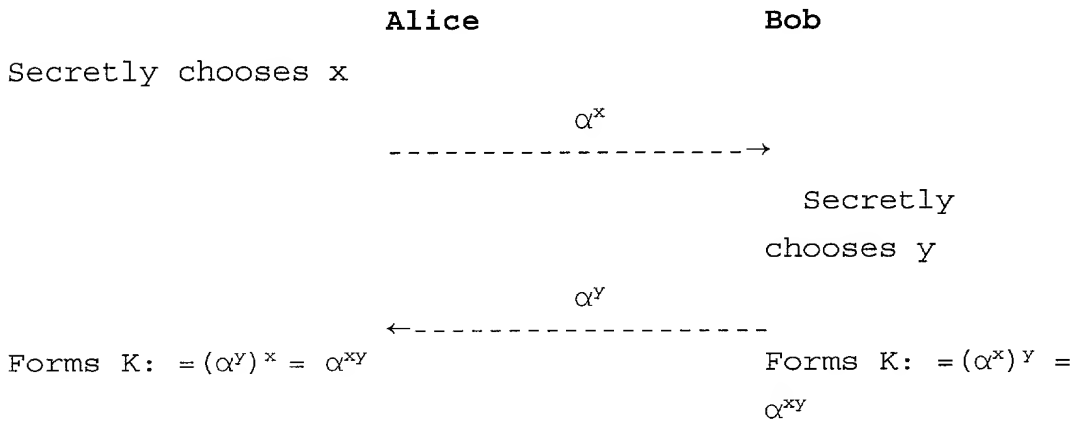
Background Information

There are many diverse encryption methods in the related art, and these methods have gained in commercial importance. They are used for transmitting information over generally accessible transmission media. However, only the owner of a cryptographic key is able to read this information in plain text.

A known method for establishing a common key via insecure communication channels is, for example, the W. Diffie and W. Hellman method (see DH method, W. Diffie and M. Hellmann; see "New Directions in Cryptography", IEEE Transactions on Information Theory, IT-22(6):644-654, November 1976).

The Diffie-Hellmann key exchange [DH76] is based on the fact that it is virtually impossible to calculate logarithms modulo a large prime number p. Alice and Bob take advantage of this fact in the example illustrated below, by each secretly choosing a number x and y, respectively, smaller than p (and prime to p-1). They then send each other (consecutively or simultaneously) the x-th (and, respectively, y-th) power of a publicly

known number α. From the received powers, they are able to calculate a common key $K:=\alpha^{xy}$ by again performing an exponentiation with x and y, respectively. An attacker, who sees only α^x and α^y, is not able to calculate K therefrom. (The [only]method known today to do so would involve first calculating the logarithm, e.g. of α^x to the base α modulo p, and then raising α^y to that power.)[ ]



Example of the Diffie-Helmann key exchange

The problem that exists in the case of the DH key exchange is that Alice does not know whether she is actually communicating with Bob or with an impostor. In IPSec, this problem is solved by the use of public key certificates in which the identity of a subscriber is [ ]linked to a public key by a trustworthy authority. In this way, the identity of a conversation partner is can be verified.

The DH key exchange can also be implemented using other mathematical structures, such as finite fields $GF(2^n)$ or elliptical curves. With such alternatives, one can improve performance.

However, this method is only suitable for agreement of a key between two subscribers.

Various attempts have been made to extend the DH method to three or more subscribers (DH groups). M. Steiner, G. Tsudik, and M. Waidner provide an overview of the state of the art in "Diffie-Hellman Key Distribution Extended to Group Communication", Proc. 3rd ACM Conference on Computer and Communications Security, March 1996, New Delhi, India.

The following table illustrates an example where the DH method is extended to three subscribers A, B and C (in each case, calculations are mod p):

	A→B	B→C	C→A
1st round	g^a	g^b	g^c
2nd round	g^{ca}	g^{ab}	g^{bc}

Once these two rounds have been carried out, each of the subscribers is able to calculate the secret key g^{abc} mod p.

In all of these extensions, at least one of the following problems occurs:

- The subscribers must be arranged in a certain manner, in the above example, for instance, in a circle.
- The subscribers have no influence on the key selection vis-à-vis the central station.
- The number of rounds is dependent on the number of subscribers.

As a general rule, these methods are difficult to implement and require substantial computational outlay.

[
]Another method for establishing a common key is known from [the]German Patent No. DE 195 38 385.0. In this

method, however, the central station must know the secret keys of the subscribers.

[An]Another approach is[also] known from Burmester, Desmedt, "A Secure and Efficient Conference Key Distribution System", Proc. EUROCRYPT'94, Springer LNCS, Berlin 1994, where two rounds are required to generate the key, it being necessary to send n communications of a length of p = approx. 1000 bits through the central station for n subscribers in the second round.

A cryptographic method described as the (n,t) threshold method is also known. In an (n,t) threshold method, a key k can be decomposed into t parts (referred to as shadows), [in such a way]so that this key k can be reconstructed from any n of the t shadows (see Beutelspacher, Schwenk, Wolfenstetter: *Moderne Verfahren der Kryptographie* (2nd edition), Vieweg Publishers, Wiesbaden, 1998).

[It is intended that the present]In IEEE Infocom '93, The Conference on Computer Communications Proceedings, Twelfth Annual Joint Conference of the IEEE Computer and Communications Societies, Networking: Foundation for the Future (cat. no. 93CH3264-9) (3/28/1993), vol. 3, pp. 1406-1413, "On the Design of Conference Key Distribution Systems for the Broadcasting Networks", a method is described for establishing a common key between a central station (chairman) and a group of n subscribers, where a threshold method is employed. In this approach, the central station (chairman) selects a common key. The method presupposes a secure channel between the chairman and the subscribers. A secure channel of this kind can be established, for example, using the DH method [DH76] indicated above, or a variant. However, for this, two communications are necessary for each subscriber, in

order to negotiate a common key between the n subscribers and the central station (chairman), and to transmit a communication around the "public shadows".

Thus, altogether 2n+1 communications are required in order to establish the common key.

Summary of the Invention

The present invention provides a method for generating a common key between a central station and a group of at least three subscribers exhibit the same standard of security as the DH method. The method can be based on a publicly known mathematical number group (G) and an element of the group $g \in G$ of a high order. Each of the n subscribers generates a random number (i), calculates the value of g^i in G, and transmits this value to the central station (Z). In the central station (Z), a random number (z) is likewise generated, and the values $(g^i)^z$ in G are calculated. From these values, the shares are derived on the basis of a threshold method and, from these, a (n,2n-1) threshold method is constructed. The central station (Z) transmits the generated shares, together with the values $(g^i)^z$, to the n subscribers, who, using the (n,2n-1) threshold method, can reconstruct the key (k). The method in accordance with the present invention can be used for generating a cryptographic key for three or more subscribers.

Detailed Description

The present invention provides a method for generating a common key between a central station and a group of at least three subscribers [have]having the same security standards as the DH method. In this context, [however,]the method [should]can be simple to implement and

require minimal computational outlay. [It should be so conceived that there is no need, in the process, for the subscribers' secret keys to be made known to the central station.

The method according to the]

The present invention is [equal to this task. It is]based, inter alia, on the same mathematical structures as the DH method and, therefore, has comparable security features. In comparison to the group DH methods proposed in known methods heretofore, it is substantially more efficient with respect to computational outlay and communication requirements.

The operating principle of the method according to the present invention is elucidated in the following. In this instance, the central station is denoted by Z, defined subscribers in the method by T1-Tn, and every single subscriber, who is not specifically named, by Ti. The publicly known components of the method include a publicly known mathematical group G, preferably the multiplicative group of all integral numbers modulo a large prime number p, and an element g of the group G, preferably a number $0<g<p$ having a high multiplicative order. For group G, however, other suitable mathematical structures can also be used, e.g., the multiplicative group of a finite field, or the group of the points of an elliptical curve.

The method [is]can be carried out in [three work steps. In the]three steps. In a first step, a communication in the form $(Ti, g^i \bmod p)$ [is]can be sent by each subscriber Ti to the central station, i being a random number of subscriber Ti selected by a random number generator.

In [the]a second work step, in central station Z:

- A random number z is generated, and the number $(g^i)^z$ mod p is calculated for each subscriber Ti.
- From these n numbers, n shares are then differentiated for n subscribers in central station Z, using a generally known (n, 2n-1) threshold method.
- n-1 further shares s^1-s^{n-1} are selected in central station Z and sent, together with the number g^z mod p, to all subscribers Tl-Tn.

In [the]a third work step, the common key k [is]can be calculated for each subscriber Ti, [

-]- $(g^z)^i$ mod p = $(g^i)^z$ mod p being calculated; [

]

- from this, a share of the threshold method being differentiated; and
- on the basis of this share and $s^1, \ldots s^{n-1}$, common key k being determined as the secret.

On the basis of a practical example, the method according to the present invention is elucidated in the following for three subscribers A, B, and C, as well as a central station Z. However, the number of subscribers can be increased to any desired number. In this example, the length of number p is 1024 bits; g has a multiplicative order of at least 2^{160}.

[T]An embodiment of the method in accordance with the present invention [is]can be carried out [in accordance with the following method steps]as follows:

- Subscribers A, B and C send g^a mod p, g^b mod p and g^c mod p to central station Z.
- g^{az} mod p, g^{bz} mod p and g^{cz} mod p are calculated in central station Z, in each case the 128 least significant bits thereof being used as shares [s]S_A, [s]S_B and, respectively, [s]S_C. In central station Z,

applying the (n,2,-1) threshold method, a 2nd degree polynomial P(x), which passes through points $(1,s_A)$, $(2,s_B)$, and $(3,s_C)$ and is uniquely defined by these points, is calculated over a finite field $GF(2^{128})$. Common key k is the point of intersection of this polynomial with the y-axis, i.e., k; =P(0). Central station Z transmits g^z mod p, s_1;=P(4) and s_2;=P(5) to subscribers A, B and C.

- For subscriber A, $(g^z)^a$ mod p is calculated. In the result, subscriber A having the 128 least significant bits of this value receives share s_A, which, together with shares s_1 and s_2 is sufficient to determine polynomial P'(x) and, thus, also key k. One proceeds analogously for subscribers B and C.

The method described above [makes do with the]<u>can use a</u> minimum number of two rounds between subscribers T1-Tn and central station Z. In contrast to the Burmester and Desmedt approach, the outlay for character strings to be transmitted by the central station to the n subscribers can be reduced in the second round to a length of 128 bits per subscriber.

[

2.]Abstract

[2.1. It is intended that t]The present invention provides a method for generating a common key between a central station and a group of subscribers, e.g., at least three subscribers, exhibit the same standard of security as the DH method.

[2.2. The method is based on a publicly known mathematical number group (G) and an element of the group $g \epsilon G$ of a high order. Each of the n subscribers generates a random number (i), calculates the value of g^i in G, and transmits this value to the central station (Z). In the central station (Z), a random number (z) is likewise generated, and the values $(g^i)^z$ in G are calculated. From these values, the shares are derived on the basis of a threshold method and, from these, a (n,2n-1) threshold method is constructed. The central station (Z) transmits the generated shares, together with the values $(g^i)^z$, to the n subscribers, who, using the (n,2n-1) threshold method, can reconstruct the key (k).]

[2.3. The method in accordance with the present invention can be advantageously used for generating a cryptographic key for a group of a plurality, however of at least three, subscribers.]

[2345/149]

DECLARATION AND POWER OF ATTORNEY

As a below named inventor, I hereby declare that:

My residence, post office address and citizenship are as stated below next to my name.

I believe I am an original, first and sole inventor of the subject matter which is claimed and for which a patent is sought on the invention entitled **METHOD FOR ESTABLISHING A COMMON KEY BETWEEN A CENTRAL STATION AND A GROUP OF SUBSCRIBERS**, the specification of which was filed as International Application No. PCT/EP99/07052 on September 22, 1999 and filed as a U.S. application having Serial No. 09/807176 on April 9, 2001 for Letters Patent in the U.S. Patent and Trademark Office.

I hereby state that I have reviewed and understand the contents of the above-identified specification, including the claims.

I acknowledge the duty to disclose information which is material to the examination of this application in accordance with Title 37, Code of Federal Regulations, § 1.56(a).

I hereby claim foreign priority benefits under Title 35, United States Code, § 119 of any foreign application(s) for patent or inventor's certificate listed below and have also identified below any foreign application(s) for patent or inventor's certificate having a filing date before that of the application on which priority is claimed:

PRIOR FOREIGN APPLICATION(S)

Number	Country Filed	Day/Month/Year	Priority Claimed Under 35 USC 119
198 479 44.1	Fed. Rep. of Germany	9 October 1998	Yes

Express Mail No. 327551813US

And I hereby appoint Richard L. Mayer (Reg. No. 22,490), Gerard A. Messina (Reg. No. 35,952) and Linda M. Shudy (Reg. No. 47,084) my attorneys with full power of substitution and revocation, to prosecute this application and to transact all business in the Patent and Trademark Office connected therewith.

Please address all communications regarding this application to:

KENYON & KENYON
One Broadway
New York, New York 10004
CUSTOMER NO. 26646

Please direct all telephone calls to Richard L. Mayer at (212) 425-7200.

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code and that such willful and false statements may jeopardize the validity of the application or any patent issued thereon.

Inventor: **Joerg SCHWENK**

Inventor's Signature: Jörg Schwenk

Date: 16.7.01

Residence: Suedwestring 27
D-64807 ~~Dieburg~~
Federal Republic of Germany

Citizenship: German

Post Office Address: Same as above.